AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions and listings of claims in the application.

LISTING OF CLAIMS

1. (Original) A communication device which is connected via a network to a session control server so as to be able to communicate with the session control server, and which establishes a session with another communication device by performing signal transmission to and reception from said session control server, comprising:

a unit which generates an asymmetric key pair;

a requesting unit which requests certificate issuance for a public key in said asymmetric key pair to said session control server;

a receiving unit which receives notification of public key certificate issuance completion from said session control server;

a storage unit which stores a public key certificate which has been received;

a sending unit which sends a registration request of the location of said communication device to said session control server; and

a receiving unit which receives notification of location registration completed, including a term of validity, from said session control server;

wherein said location registration request and said certificate issuance request are sent as a combined request.

2. (Original) A communication device according to claim 1, wherein said storage unit which stores said public key certificate stores a term of validity which are included in a location registration completed notification as the term of validity of the certificate which is issued.

3. (Original) A communication device which is connected via a network to a session control server so as to be able to communicate with the session control server, and which establishes a session with another communication device by performing signal transmission to and reception from said session control server, comprising:

a unit which generates an asymmetric key pair;

a storage unit which stores a public key certificate from among said asymmetric key pair;

a sending unit which sends a registration request of said public key certificate to said session control server;

a sending unit which sends a registration request of the location of said communication device to said session control server; and

a receiving unit which receives notification of location registration completed, including a term of validity, from said session control server.

4. (Original) A communication device according to claim 3, wherein said storage unit which stores said public key certificate stores a term of validity which are included in a location registration completed notification as the term of validity of the certificate which is issued.

5. (Original) A session control server which is connected via a network to a plurality of communication devices so as to be able to communicate with the communication devices, and which, by receiving a signal which is sent from a communication device on a signal originating side, and sending the signal which it

has received to a communication device on the signal reception side, establishes a session between said communication device on the signal originating side and said communication device on the signal reception side, comprising:

a receiving unit which receives a location registration request from said communication device, and a certificate issuance request or a certificate registration request for a public key, as a combined request;

a unit which receives said request, and which performs issuance of a public key certificate, or confirms the validity of said public key certificate; and

a unit which stores said public key certificate which has been issued or registered and location information, along with a term of validity.

6. (Original) A session control server according to claim 5, further comprising:

a receiving unit which receives an inquiry request for said public key certificate; and

a sending unit which notifies said public key certificate, after having confirmed the validity of said public key certificate.

7. (Original) A communication system for mutually establishing a session with a communication device, and which is connected via a network so as to be capable of communication, comprising:

a communication device which comprises a mean which generates an asymmetric key pair, a requesting unit which performs a request for issuance of a certificate for a public key, a receiving unit which receives notification of certificate issuance, a storage unit which stores a public key certificate, a sending unit which

sends a location registration request, and a unit which receives a location registration completed notification which includes a term of validity; and

a session control server which comprises a receiving unit which receives a location registration request from said communication device, a receiving unit which receives a combination of a request for certificate issuance or certificate registration for a public key, a unit which issues a certificate or confirms the validity of a certificate, and a storage unit which stores a certificate which has been issued or registered and location information together with an expiry.

8. (Original) A communication system according to claim 7, wherein

said communication device comprises a storage unit which stores a term of validity which is included in a location registration completed notification as a term of validity of a public key certificate which has been issued, and

said session control server comprises a receiving unit which receives a certificate inquiry request, and a unit which sends a certificate notification.

9. (Original) A communication system according to claim 7, wherein

said communication device comprises a unit which stores an asymmetric key pair, and a sending unit which sends a registration request for a public key certificate; and

said session control server comprises a receiving unit which receives a certificate inquiry request, and a sending unit for a certificate notification.

10. (Original) A communication method for mutually establishing a session with a communication device, which is connected via a network so as to be capable of communication, wherein:

a session control server, when it receives a request signal from a communication device for location registration and certificate issuance, determines the type of the signal, and, if it is a location registration request, makes a decision as to whether or not it includes a certificate issuance request, and, if an issuance request is included within said signal, issues a certificate, and along with managing said location information and said certificate, sends a signal for location information and certificate issuance completion to said communication device.

11. (Original) A communication method for mutually establishing a session with a communication device, which is connected via a network so as to be capable of communication, wherein:

a session control server, when it receives a certificate query request signal from a communication device, along with performing session control, decides whether or not it is addressed to its own domain, and, if it is addressed to its own domain, determines the type of the signal, and if it is a certificate query request, decides whether or not a certificate is present, and if there is a certificate, searches a corresponding certificate, confirms the validity of the certificate which has been searched, and sends a certificate notification to said communication device; while, if it is not addressed to its own domain, it transfers said certificate query request signal to the destination session control server.

12. (Original) A program for communication for mutually establishing a session with a communication device, which is connected via a network so as to be capable of communication, for causing a computer of a session control server to execute:

a procedure of receiving a request signal for location registration and certificate issuance from a communication device; a procedure of determining the type of the signal; a procedure of, if it is a location registration request, deciding whether or not it includes a certificate issuance request; a procedure of, if it includes an issuance request, issuing a certificate; a procedure of managing said location information and said certificate; and a procedure of sending a signal of location information and certificate issuance completion notification to said communication device.

13. (Original) A program for communication for mutually establishing a session with a communication device, which is connected via a network so as to be capable of communication, for causing a computer of a session control server to execute:

a procedure of receiving a request signal for location registration and certificate issuance from a communication device; a procedure of performing session control; a procedure of deciding whether or not it is addressed to its own domain; a procedure of, if it is addressed to its own domain, determining the type of the signal; a procedure of, if it is a certificate query request, determining whether or not there is a certificate; a procedure of, if there is a certificate, searching a corresponding certificate; a procedure of confirming the validity of a certificate which has been searched; and a procedure of sending a certificate notification to said communication device; and a procedure of, if it is not addressed to its own domain, transferring said certificate query request signal to the destination session control server.

14. (Original) A computer readable recording medium, in which a program for communication according to claim 12 is recorded.

15. (Original) A computer readable recording medium, in which a program for communication according to claim 13 is recorded.

16. – 36. (Cancelled)

37. (Original) A communication device which is connected via a network with a session control server so as to be able to perform communication, and which establishes a session with another communication device by performing signal transmission and reception with said another communication device via at least one of said session control server, comprising:

a mean which, when sending information which is encrypted in order to maintain confidentiality of the sent signal, generates a first encryption key for encryption;

a unit which encrypts the information by using said first encryption key;

a unit which encrypts said first encryption key using an arbitrary second encryption key; and

a mean which sends a signal which includes the information which has been encrypted with said first encryption key, to which said first encryption key which has been encrypted is attached,

wherein the unit which encrypts said first encryption key with the second encryption key encrypts the first encryption key with the second encryption key of a

single session control server which is permitted only reference to the information within the signal, or which is permitted both reference and modification; and

the unit which sends the information which has been encrypted with said first encryption key sends said first encryption key which has been encrypted, the information which has been encrypted with said first encryption key, and a decryption request command to said session control server, or a decryption request command and a change permission notification.

38. (Original) A session control server which is connected via a network to a plurality of communication devices so as to be able to communicate with the communication devices and to another session control server, and which, by receiving a signal which is sent from a communication device on a signal originating side or said another session control server, and sending the signal which it has received to a communication device on a signal reception side or said another session control server, establishes a session between said communication device on the signal originating side and said communication device on the signal reception side, comprising:

a unit which receives a signal which includes information to which a first encryption key which has been encrypted is attached, and which has been encrypted with said first encryption key;

a unit which decrypts the first encryption key with a second decryption key which corresponds to its own second encryption key;

a unit which decrypts the information using the first encryption key which has been obtained by decryption;

a unit which encrypts the first encryption key which has been obtained by decryption with an arbitrary second encryption key; and

a unit which sends a signal which includes information which has been encrypted with the first encryption key which has been obtained by decryption, and attaches the first encryption key which has been obtained by decryption, after it has been encrypted with the arbitrary second encryption key,

wherein, when said receiving unit receives the signal which includes the information which has been encrypted, obtains said first encryption key by making a decision as to the presence or absence of a decryption request and obtaining said first encryption key by decrypting the encryption key with a second decryption key which corresponds to said second encryption key, or by decrypting said encryption key with a second decryption key which corresponds to said second encryption key and making a decision as to the presence or absence of a decryption request, or by performing both thereof;

said information decryption unit decrypts the information which has encrypted with said first encryption key; and

said encryption unit encrypts the first encryption key which has been obtained with a second encryption key of said another session control server which passes through during transmission and reception, and which are permitted with either only reference, or both reference and modification, or with a second encryption key of a transmission destination communication device; and

said sending unit sends said first encryption key which has been encrypted, the information which has been encrypted with the first encryption key which has been obtained, and, if the second encryption key is an encryption key of said another session control server, a decryption request command, or a decryption request

command and an alteration permit notification, for said another session control server.

39. (Original) A session control server according to claim 38, wherein in addition to said unit, further includes:

a unit which, when sending a signal which includes information which is encrypted in order to preserve the confidentiality of the sent signal, generates a new first encryption key for encryption;

a unit which encrypts the information using said first encryption key which has been generated;

a unit which encrypts said first encryption key which has been generated by using an arbitrary second encryption key; and

a unit which sends a signal to which said first encryption key which has been generated and which has been encrypted with said second encryption key is attached, and which includes the information which has been encrypted with said first encryption key which has been generated,

wherein the encryption unit for said first encryption key encrypts the first encryption key which has been obtained with a second encryption key of said another session control server which passes through during transmission and reception, and which are permitted with either only reference, or both reference and modification, or with a second encryption key of a transmission destination communication device; and

said sending unit sends said first encryption key which has been generated and encrypted, the information which has been encrypted with the first encryption key which has been generated, and, if the second encryption key is an encryption

key of said another session control server, a decryption request command, or a decryption request command and an alteration permit notification, for said another session control server.

40. (Original) A session control server according to claim 38, further comprising:

a unit which stores said first encryption key by session and opposing device; and

a reuse unit which reuses said first encryption key in the same session, at least one of encryption and decryption of information in the same opposing device.

41. (Original) A communication device which is connected via a network with a session control server so as to be able to perform communication, and which establishes a session with another communication device by performing signal transmission and reception with said session control server, comprising:

a unit which receives a signal to which a first encryption key which has been encrypted is attached, and which includes information which has been encrypted;

a unit which decrypts said first encryption key;

a unit which decrypts the information with said first encryption key;

a unit which stores said first encryption key by session and opposing device;

a unit which encrypts information using said first encryption key; and

a unit which sends a signal which includes the information which has been encrypted with said first encryption key,

wherein said first encryption key which has been stored in said storage unit is employed for at least one of encryption and decryption of information within the same session.

42. (Original) A communication device according to claim 37, further comprising:

a unit which stores said first encryption key by session and opposing device;

a unit which encrypts information by using said first encryption key;

a unit which sends a signal which includes the information which has been encrypted with said first encryption key;

a unit which receives a signal which includes information which has been encrypted with said first encryption key; and

a unit which decrypts the information by using said first encryption key,

wherein said first encryption key which has been stored in said storage unit is employed for at least one of encryption and decryption of information within the same session.

43. (Original) A communication device according to claim 37, further comprising a unit which periodically updates said first encryption key which is managed by session and opposing device,

wherein said updating unit comprises:

a unit which newly generates a first encryption key;

an encryption key encryption unit which encrypts said first encryption key with an arbitrary second encryption key, or with a first encryption key which is already stored; and

a unit which sends a signal to which is attached said first encryption key which has been encrypted with the arbitrary second encryption key, and which includes information which has been encrypted with said first encryption key.

44. (Original) A communication device according to claim 41, further comprising a unit which periodically updates said first encryption key which is managed by session and opposing device,

wherein said updating unit comprises:

a unit which newly generates a first encryption key;

an encryption key encryption unit which encrypts said first encryption key with an arbitrary second encryption key, or with a first encryption key which is already stored; and

a unit which sends a signal to which is attached said first encryption key which has been encrypted with the arbitrary second encryption key, and which includes information which has been encrypted with said first encryption key.

45. (Original) A session control server according to claim 37, further comprising:

a unit which periodically updates said first encryption key which is managed by session and opposing device;

a unit which receives a signal which includes information which has been encrypted with said first encryption key, and to which is attached a new first encryption key which has been encrypted with an arbitrary second encryption key, or with the first encryption key which is already stored;

a unit which encrypts information using the new first encryption key which has been updated; and

a unit which sends the new encryption key which has been updated, together with the encrypted information,

wherein said sending unit sends the information which has been encrypted with said first encryption key, and attaches the new first encryption key which has

been encrypted with said desired second encryption key, or with said first encryption key which is already stored.

46. (Original) A session control server according to claim 38, comprising:

a unit which periodically updates the first encryption key which is managed by session and said opposing device;

a unit which receives a signal, with a new first encryption key attached which has been encrypted with an arbitrary second encryption key or with a first encryption key which is already stored, which includes information which has been encrypted with said first encryption key;

a unit which encrypts information by using the first encryption key which has newly been updated; and

a unit which sends the first encryption key which has newly been updated, along with the encrypted information,

wherein said sending unit sends the signal, with said new first encryption key attached which has been encrypted with said an arbitrary second encryption key or with said first encryption key which is already stored, which includes information which has been encrypted with said first encryption key.

47. (Original) A communication system which is connected via a network so as to be able to perform communication each other, and which establishes a session by performing mutual signal send and reception with a communication device, comprising:

a unit which receives a signal to which a first encryption key which has been encrypted is attached, and which includes information which has been encrypted

with said first encryption key; a unit which decrypts the first encryption key with a second decryption key which corresponds to its own second encryption key; a unit which decrypts the information by using the first encryption key which has been obtained by decryption; a unit which encrypts the first encryption key which has been obtained by decryption using an arbitrary second encryption key; and a unit which, after having performed encryption with the arbitrary second encryption key, sends a signal, with said first encryption key which has been obtained by decryption attached, which includes information which has been encrypted with said first encryption key which has been obtained by decryption,

wherein a session control server which, when said receiving unit receives the signal which includes the information which has been encrypted, obtains said first encryption key by making a decision as to the presence or absence of a decryption request and by decrypting the encryption key with a second decryption key which corresponds to said second encryption key, or by decrypting said encryption key with a second decryption key which corresponds to said second encryption key and making a decision as to the presence or absence of a decryption request, or by performing both thereof; decrypts the information which said information decryption unit has encrypted with said first encryption key; wherein said encryption unit encrypts the first encryption key which has been obtained with a second encryption key of said another session control server which passes through during transmission and reception, and which are permitted with either only reference, or both reference and modification, or with a second encryption key of a transmission destination communication device; and said sending unit sends said first encryption key which has been encrypted, the information which has been encrypted with the first encryption key which has been obtained, and, if the second encryption key is an

encryption key of said another session control server, a decryption request command for said another session control server;

a communication device which comprises: a unit which, when sending a signal which includes information which is encrypted in order to preserve the confidentiality of the sent signal, generates a new first encryption key for encryption; a unit which encrypts the information by using said first encryption key for encryption; a unit which encrypts said first encryption key by using an arbitrary second encryption key; and a unit which sends a signal to which said first encryption key which has been encrypted is attached, and which includes the information which has been encrypted with said first encryption key, wherein the unit which encrypts said first encryption key with the second encryption key encrypts the first encryption key with a second encryption key of said another session control server on which either only reference, or both reference and modification, are permitted, or with a second encryption key of a transmission destination communication device; and the unit which sends a signal which includes the information which has been encrypted with said first encryption key sends said first encryption key which has been encrypted, the information which has been encrypted with the first encryption key, and, if said second encryption key is an encryption key of said session control server, a decryption request command to said session control server;

or a communication device which, in addition to said unit, comprises: a unit which, when sending a signal which includes information which is encrypted in order to preserve the confidentiality of the sent signal, generates a new first encryption key for encryption; a unit which encrypts the information by using said first encryption key for encryption which has been generated; a unit which encrypts said first encryption key which has been generated by using an arbitrary second encryption key; and a

unit which sends a signal to which said first encryption key which has been generated and which has been encrypted with said second encryption key is attached, and which includes the information which has been encrypted with said first encryption key which has been generated, wherein the unit which encrypts said first encryption key encrypts said first encryption key which has been generated with a second encryption key of an another session control server which passes through during transmission and reception, and which are permitted with either only reference, or both reference and modification, or with a second encryption key of a transmission destination communication device; and said sending unit sends said first encryption key which has been generated and encrypted, the information which has been encrypted with said first encryption key which has been generated, and, if the second encryption key is an encryption key of said another session control server, a decryption request command for said another session control server;

a unit which receives a signal which includes the information which has been encrypted, to which the first encryption key which has been encrypted is attached, and which includes the information which has been encrypted;

a signal reception side communication device which comprises a unit which decrypts said first encryption key, a unit which decrypts the information with said first encryption key, a unit which stores said first encryption key by session and opposing device unit, a unit which encrypts information by using said first encryption key, and a unit which sends a signal which includes the information which has been encrypted by using said first encryption key, wherein said first encryption key which has been stored in said storage unit is employed for at least one of encryption and decryption of information in the same session; and

a signal originating side communication device which comprises a unit which stores said first encryption key by session and opposing device unit, a unit which encrypts information by using said first encryption key, a unit which sends a signal which includes the information which has been encrypted by using said first encryption key, a unit which receives a signal which includes information which has been encrypted by using said first encryption key, and a unit which decrypts the information by using said first encryption key, wherein said first encryption key which has been stored in said storage unit is employed for at least one of encryption and decryption of information in the same session.

48. (Original) A communication system according to claim 47, comprising:

a session control server which comprises a unit which stores said first encryption key by session and opposing device; and a reuse unit which reuses said first encryption key for at least one of encryption and decryption of information the same session and in the same opposing device;

a signal reception side communication device which comprises a unit which receives an encrypted signal to which the first encryption key which has been encrypted is attached, and which includes the information which has been encrypted, a unit which decrypts said first encryption key, a unit which decrypts the information with said first encryption key, a unit which stores said first encryption key by session and opposing device unit, a unit which encrypts information by using said first encryption key, and a unit which sends a signal which includes the information which has been encrypted by using said first encryption key, wherein said first encryption key which has been stored in said storage unit is employed for at least one of encryption and decryption of information in the same session; and

and a signal originating side communication device which comprises a signal originating side communication device which comprises a unit which stores said first encryption key by session and opposing device unit, a unit which encrypts information by using said first encryption key, a unit which sends a signal which includes the information which has been encrypted by using said first encryption key, a unit which receives a signal which includes information which has been encrypted by using said first encryption key, and a unit which decrypts the information by using said first encryption key, wherein said first encryption key which has been stored in said storage unit is employed for at least one of encryption and decryption of information in the same session.

49. (Original) A communication system according to claim 47, comprising:

a session control server which comprises: a unit which periodically updates the first encryption key which is managed by session and said opposing device; a unit which receives a signal, with a new first encryption key attached which has been encrypted with an arbitrary second encryption key or with a first encryption key which is already stored, which includes information which has been encrypted with said first encryption key; a unit which encrypts information by using the first encryption key which has newly been updated; and a unit which sends the first encryption key which has newly been updated, along with the encrypted information, wherein said sending unit sends the signal, with said new first encryption key attached which has been encrypted with said an arbitrary second encryption key attached which has been encrypted with said an arbitrary second encryption key or with said first encryption key which is already stored, which includes information which has been encrypted with said first encryption key;

a signal originating side communication device which comprises: a unit which stores said first encryption key by session and opposing device unit, a unit which encrypts information by using said first encryption key, a unit which sends a signal which includes the information which has been encrypted by using said first encryption key, a unit which receives a signal which includes information which has been encrypted by using said first encryption key, and a unit which decrypts the information by using said first encryption key, wherein said first encryption key which has been stored in said storage unit is employed for at least one of encryption and decryption of information in the same session; and

a signal originating side or signal reception side communication device which comprises a unit which periodically updates the first encryption key which is managed by session and said opposing device, wherein said updating unit comprises a unit which newly generates the first encryption key, an encryption key encryption unit which encrypts said first encryption key with an arbitrary second encryption key, and a unit which sends a signal, with said new first encryption key attached which has been encrypted with said an arbitrary second encryption key, which includes information which has been encrypted with said first encryption key.

50. (Original) A communication method which sends a session control signal which is generated by a signal originating side communication device to a signal reception side communication device via a session control server which is trusted, and a session control server which is not trusted, wherein:

said signal originating side communication device encrypts a first encryption key which is used for encryption with a second encryption key of a session control server which has been made public;

a value which indicates a decryption request to said session control server, and a contents ID which is to be decrypted, are sent together;

said session control server decides upon a decryption request according to the value of a decryption request parameter, or decides upon a decryption request according to whether it is possible or impossible to decrypt data in which the first encryption key which has been encrypted is set;

if there is a decryption request, it is decrypted with a second decryption key which corresponds to the second encryption key, and reference to or change of the control information between the control devices is made possible;

after having changed the control information between the communication devices, the information after change is encrypted either by employing said first encryption key just as it is, or using a first encryption key which has been newly generated; and

the information after change is sent to a next session control server, or to a signal reception side communication device.

51. (Original) A communication method in which a session control server changes the filtering conditions of a NAT/firewall device based upon information which has been obtained during establishment of a session, wherein:

the session control server, after having determined a decryption key for decryption, decrypts a first encryption key, and decrypts encrypted information with said first encryption key, thus making it possible to refer to or to change control information between communication devices;

based upon said control information, change of the filtering conditions is requested to the NAT/firewall device;

thereafter, control information between communication devices which has been received from a signal reception side communication device is decrypted, and it is made possible to refer to, or to change, the control information between communication devices; and

based upon said control information, change of the filtering conditions is requested to the NAT/firewall device, and mutual packet passage for main information between communication devices is performed by the NAT/firewall device.

52. (Original) A communication method in which a session control server makes it possible to record communication of main information which has been encrypted, based upon information which has been obtained during establishment of a session, wherein:

a session control server, in addition to a request to change filtering conditions to a NAT/firewall device or the like, commands main information transfer, and, when main information is received from the NAT/firewall device or the like, if said main information is encrypted, when transmitting and receiving a signal, decrypts a first encryption key, and decrypts the encrypted information, along with control information between communication devices which has been obtained by decrypting with said first encryption key, by using a key for main information encryption, which has already been obtained, and records said main information in a communication recording unit.

53. (Original) A program for communication which sends a session control signal which has been generated by a signal originating side communication device to a

signal reception side communication device via a session control server which is trusted and a session control server which is not trusted, for causing a computer of said session control server to execute:

a procedure of deciding upon a decryption request according to the value of a decryption request parameter, or deciding upon a decryption request according to whether it is possible or impossible to decrypt data in which a first encryption key which has been encrypted is set; a procedure of, if there is a decryption request, decrypting it with a second decryption key which corresponds to the second encryption key, and making reference to or change of the control information between the control devices possible; a procedure of encrypting the information after change either by employing said first encryption key just as it is, or using a first encryption key which has been newly generated; and a procedure of sending it to a next session control server, or to a signal reception side communication device.

54. (Original) A program for communication which causes a session control server to change the filtering conditions of a NAT/firewall device, based upon information which has been obtained during establishment of a session, for causing a computer of said session control server to execute:

a procedure of determining a decryption key for decryption; a procedure of performing decryption of a first encryption key; a procedure of decrypting encrypted information with said first encryption key, thus making it possible to refer to or to change control information between communication devices; a procedure of, based upon said control information, requesting change of the filtering conditions to the NAT/firewall device; a procedure of, thereafter, decrypting control information between communication devices which has been received from a signal reception

side communication device, and making it possible to refer to, or to change, the control information between communication devices; and a procedure of, based upon said control information, requesting change of the filtering conditions to the NAT/firewall device

55. (Original) A program for communication which causes a session control server to perform recording of communication of main information which has been encrypted, based upon information which has been obtained during establishment of a session, for causing a computer of said session control server to execute:

a procedure of, in addition to a request to change filtering conditions to a NAT/firewall device or the like, commanding main information transfer; a procedure of receiving main information from the NAT/firewall device or the like; a procedure of, if said main information is encrypted, when transmitting and receiving a signal, performing decryption of a first encryption key, and decrypting the encrypted information, along with control information between communication devices which has been obtained by decrypting with said first encryption key, by using a key for main information encryption, which has already been obtained; and a procedure of recording said main information in a communication recording unit.

56. (Original) A computer readable recording medium, in which a program for communication according to claim 53 is recorded.

57. (Original) A computer readable recording medium, in which a program for communication according to claim 54 is recorded.

58. (Original) A computer readable recording medium, in which a program for communication according to claim 55 is recorded.